AUTHENTICATION METHOD AND APPARATUS AT WIRELESS LAN SYSTEM

BACKGROUND OF THE INVENTION

The present invention relates to an authentication method and apparatus at a wireless LAN (local area network) system, in particular, based on the IEEE (Institute of Electrical and Electronics Engineers) 802.11.

Description of the Related Art

A wireless LAN system based on the IEEE 802.11 has been developed. In the system, frequency bands such as 2.4 GHz or 5 GHz can be used without license, therefore, it is important to keep security at the wireless network.

At the chapter 8, Authentication and Privacy, in the IEEE 802.11, Open system authentication method and Shared key authentication method used WEP (wired equivalent privacy) algorithm are stipulated, and either one of the Authentication methods is fixed and used in a wireless LAN system.

Fig. 1 is a block diagram showing a conventional structure of a wireless LAN system based on the IEEE 802.11. In Fig. 1, a STA 1 is a terminal station and the plural STAs 1 are provided in the wireless LAN system, and each STA 1 is a data terminal having transmitting and receiving functions for radio signals, such as a notebook size PC (personal computer).

And an AP (access point) 2 has an interface function between a wireless network and a wired network, and also has transmitting and receiving functions for radio signals, and further provides firmware for controlling the radio signals and a MAC (medium access control) address authentication function. And plural APs 2 are also provided in the wireless LAN system. A maintenance server 4 sets and controls the plural APs 2 by a SNMP (simple network management protocol).

The connection between the STAs 1 and the APs 2 is a wireless network 5, and the connection between the APs 2 and the maintenance server 4 is a wired network such as Ethernet.

First, referring to a drawing, the shared key authentication method is explained. Fig. 2 is a sequence diagram showing a conventional procedure of encryption authentication used the WEP algorithm stipulated in the IEEE 802.11. In Fig.2, the encryption authentication used the WEP algorithm is executed in a MAC (media access control) being a sub-layer of a data link layer that is the second layer of an OSI (open system interconnection).

The MAC controls access rights when data transmission requests from plural terminal stations compete with one another on a common transmission line, and distinguishes physical connecting points between the terminal stations and the transmission line, and forms frames, and executes error control on the transmission line, together with a physical layer being the first layer of the OSI.

First, an authentication request is transmitted from a STA 1 to an AP 2 by a radio signal (S1). At this time, bits showing the authentication request based on the shared key authentication method are provided in a PDU (packet data unit) format. And a MAC address of the STA 1 is included in a MAC frame as a source address.

Next, a challenge text is transmitted from the AP 2, which is received the authentication request, to the STA 1 (S2). The STA 1 encrypts the received challenge text by using the own shared key and an IV (initialization vector) based on the WEP algorithm (S3).

And the STA 1 transmits the encrypted challenge text and the IV to the AP 2 (S4). The AP 2 decrypts the received encrypted challenge text by using the received encrypted challenge text, the IV, and the own shared key. And the AP 2 compares the challenge text transmitted at the S2 with the decrypted challenge text obtained at the S4, and judges whether the two challenge texts are the same or not (S5).

When the judged result is the same, the AP 2 transmits a successful code as an authentication completed notice to the STA 1, because the authentication has completed (S6). The STA 1 received the authentication completed notice transfers to association operation with the AP 2 (S7).

At the open system authentication method, when the STA 1 transmits an authentication request to the AP 2, any special judging procedure is not executed, and an authentication result is transmitted from the AP 2 to the STA 1. This is a simple procedure.

However, at the conventional wireless LAN system based on the IEEE 802.11, the authentication method and apparatus have the following problems.

First, at the conventional wireless LAN system mentioned above, the AP 2 authenticates the MAC address. However, generally the main task of the AP 2 is an interface function between the wireless network and the wired network, therefore there is a limit in hardware and software to execute the authentication function of the MAC address. Especially, it is difficult for the generally used AP 2 to provide a MAC address table of many STAs 1, for example, more than 10000 STAs 1. Consequently, authenticating the MAC addresses for the many STAs 1 becomes difficult.

Second, a card such as a PC card, in which hardware and firmware for controlling radio signals and an ID (identifier) are memorized, has been recently used in each terminal station in the wireless LAN system. In order to apply the shared key authentication method stipulated in the IEEE 802.11 to this kind wireless LAN system, the shared key is also memorized in the card. In this case, the card is small and easy to carry, and forgetting to leave the key or stolen the key will happen, therefore the probability that the key is used illegally becomes large, and a method to keep the security is required.

Thirdly, after the authentication procedure is completed at the open system authentication method, the communication period after the association has no limitation, consequently, there is a possibility to be connected illegally, and the security becomes low.

SUMMARY OF THE INVENTION

It is therefore an object of the present invention to provide an authentication method and apparatus at a wireless LAN system, which can keep the security.

According to the present invention, for achieving the object mentioned above, there is provided an authentication method at a wireless LAN (local area network) system. The authentication method provides the steps of; transmitting an authentication request from a STA (terminal station) to an AP (access point), with which the STA desires to make association, requesting authentication of the authentication request from the AP to an authentication server, by converting the authentication request to a protocol adaptable to the authentication server, cheking the authentication request at the authentication server based on a MAC (media access control) address of the STA, executing encryption authentication at the AP with the STA based on a designated encryption algorithm, and notifying an authentication completion from the authentication server to the AP, after the authentication server received a response of a completion of the encryption authentication from the AP.

According to the present invention, after the encryption authentication is normally completed, a table of the MAC address in the AP is renewed by an instruction from the authentication server.

According to the present invention, in case that a trouble occurs at the authentication server, the AP itself executes authentication of the

MAC address.

According to the present invention, the encryption algorithm uses a shared key having a predetermined usable period.

According to the present invention, in case that the predetermined usable period of the shared key expired, the MAC address is authenticated by an open system authentication method, and at the open system authentication method, after association, a period of communication is limited to a designated short time, and a key is transported in the limited time by using such an Internet Key Exchange method of Public Key Infrastructure, and the authentication request is executed again by using the shared key.

According to the present invention, the authentication algorithm is a WEP (wired equivalent privacy) algorithm stipulated in the IEEE 802.11.

BRIEF DESCRIPTION OF THE DRAWINGS

The objects and features of the present invention will become more apparent from the consideration of the following detailed description taken in conjunction with the accompanying drawings in which:

Fig. 1 is a block diagram showing a conventional structure of a wireless LAN system based on the IEEE 802.11;

Fig. 2 is a sequence diagram showing a conventional procedure of encryption authentication used the WEP algorithm stipulated in the IEEE 802.11;

Fig. 3 is block diagram showing a system structure of an embodiment of an authentication apparatus of a wireless LAN system of the present invention;

Fig. 4 is a diagram showing a protocol stack at each node of a control plane of the embodiment of the authentication apparatus of the wireless LAN system of the present invention;

Fig. 5 is a sequence diagram showing an authentication procedure of a first embodiment of an authentication method of the wireless LAN system of the present invention;

Fig. 6 is a sequence diagram showing an authentication procedure of a third embodiment of the authentication method of the wireless LAN system of the present invention.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawings, embodiments of the present invention are explained in detail. Fig. 3 is block diagram showing a system structure of an embodiment of an authentication apparatus of a wireless LAN system of the present invention. In Fig. 3, a STA 1 is a terminal station and the plural STAs 1 are provided in the authentication apparatus of the wireless LAN system of the present invention. Each STA 1 consists of a data terminal 10 such as a notebook size PC, and a wireless LAN card 20 in which hardware and firmware for transmitting and receiving radio signals and for controlling the radio signals are provided.

And an AP 2 has an interface function between a wireless network and a wired network, and also provides hardware and firmware for transmitting and receiving radio signals and for controlling the radio signals. And the AP 2 also provides a function for converting protocols so that the authentication protocol of the IEEE 802.11 and the protocol to authenticate the STA 1 are made to be adaptable to the authentication protocol of an authentication server. The plural APs 2 are also provided in the authentication apparatus of the wireless LAN system of the present invention.

An authentication server 3 is a server having an authentication function, and usable MAC addresses of the STAs 1 are registered in the authentication server 3 beforehand. At the embodiment of the present invention, a RADIUS (remote authentication dial in user service) server having functions such as access for dialing up, authentication, and charging is used. However, the authentication server 3 is not limited to the RADIUS server. And the authentication server 3 also has a function for executing the MAC address authentication by connecting to the APs 2.

A maintenance server 4 is a server to set and control the APs 2 by the SNMP.

At the embodiment of the present invention, the authentication server 3 and the maintenance server 4 are separated and independent, however, both functions can be installed in one server.

The connection between the STAs 1 and the APs 2 is a wireless network 5, and the connection between the APs 2 and the authentication server 3, and between the APs 2 and the maintenance server 4 is a wired network 6 such as Ethernet.

Fig. 4 is a diagram showing a protocol stack at each node of a control plane of the embodiment of the authentication apparatus of the wireless LAN system of the present invention.

In Fig.4, at the IEEE 802.11, the association and the authentication are handled as entities in the MAC being the sub layer of the data link layer. In the wireless network 5, encryption authentication is executed based on the IEEE 802.11. When the AP 2 receives an authentication request from the wireless network 5, the AP 2 transfers the authentication request to the authentication server 3. The authentication server 3 executes authentication operation by using the RADIUS protocol.

Fig. 5 is a sequence diagram showing an authentication procedure of a first embodiment of an authentication method of the wireless LAN system of the present invention. At the embodiment of the present invention, in addition to the encryption authentication used the shared key authentication method utilized the WEP algorithm stipulated in the IEEE 802.11, an authentication used the MAC address is executed.

Keys of the STAs 1 and the APs 2 are set beforehand, and usable MAC addresses of the STAs 1 are registered in the authentication server 3 beforehand.

As explained in Fig. 3, at the embodiment of the authentication apparatus of the wireless LAN system of the present invention, the wireless LAN card 20 is provided in the STA 1, consequently, there is a possibility that the wireless LAN card is forgotten to leave, or the card is stolen by an illegal user and used. Therefore, in order to keep the security in a high level, the authentication used the MAC address is combined with the shared key authentication method to determine which cards are stolen. In Fig. 5, a procedure that is the same procedure in Fig. 2 has the same reference number.

Referring to Fig. 5, operation of the embodiment of the authentication apparatus of the wireless LAN system of the present invention is explained. First, an authentication request is transmitted from a STA 1 to an AP 2 by a radio signal (S1). At this time, bits showing the authentication request based on the shared key authentication method are provided in the PDU format. And a MAC address of the STA 1 is included in a MAC frame as a source address.

At the conventional WEP algorithm shown in Fig.2, the AP 2 received the authentication request provides a challenge text and transmits the challenge text to the STA 1. However, at the first embodiment of the present invention, the AP 2 requests a check to the authentication server 3 by using the MAC address as the ID (identifier) (S8).

In this, the authentication server 3 is a RADIUS server, and operates based on the RADIUS protocol defined by the RFC (request for comments) 2138 of the IETF (Internet engineering task force).

And the MAC address is defined as a user name or a calling-station ID on the authentication protocol (RADIUS protocol).

The authentication server (RADIUS server) 3 checks the MAC address received from the AP 2 (S9).

In case that the MAC address is checked and confirmed, a challenge message is transmitted to the AP 2, base on a procedure being equivalent to the CHAP (PPP challenge handshake authentication protocol) defined at the RFC 1994 of the IETF (S10). In this, the PPP signifies a point-to-point protocol.

At the CHAP, a message digest 5 (MD 5) is defined as a hashing method being one way. However, instead of the MD 5, one of the other hashing methods can be used.

The AP 2 received the challenge message from the authentication server 3 transmits a challenge text to the STA 1 based on the normal WEP algorithm (S2). As the challenge text, the challenge message transmitted from the authentication server 3 can be used as it is, instead of the challenge text based on the WEP algorithm.

The STA 1 encrypts the challenge text received from the AP 2 by using the own shared key and an IV based on the WEP algorithm (S3).

And the STA 1 transmits the encrypted challenge text and the IV to the AP 2 (S4). The AP 2 decrypts the received encrypted challenge text by using the received encrypted challenge text, the IV, and the own shared key. And the AP 2 compares the challenge text transmitted at the S2 with the decrypted challenge text obtained at the S4, and judges whether the two challenge texts are the same or not, and when the judged result is the same, the authentication at the wireless network is success (S5).

The AP 2 returns a CHAP response (challenge response) to the authentication server 3 by hashing of the CHAP (S11).

When the authentication server 3 acknowledges that a normal response is received by using the CHAP, the authentication server 3 notifies the completion of the authentication (successful code) to the AP 2 by judging that the total authentication is completed (S12).

The AP 2, received the authentication completion notification (successful code), notifies the authentication completion to the STA 1, and the STA 1 also recognizes that the authentication is successful (S6).

The authentication server 3 instructs that the usable MAC address table stored in the AP 2 is made to renew (S13). As a result, a newly authenticated MAC address is registered at any time, and the MAC address table in the AP 2 can be automatically renewed. After this operation, the STA 1 and the AP 2 go to association operation (S7).

As a result of the first embodiment, the following effect can be also realized. At the first embodiment of the present invention, as shown in Fig. 5, the AP 2 executes the authentication request to the authentication server 3 by using the MAC address as the ID (S8). However, when a trouble occurs at the hardware or the software in the authentication server 3 and the authentication server 3 can not receive the authentication request from the AP 2, at that time, the AP 2 itself can execute the authentication by using the MAC address.

As mentioned at the S 13 in Fig. 5, the MAC address table in the AP 2 is automatically renewed, therefore the authenticated result is taken in the MAC address table in the AP 2 immediately. The AP 2 stores the MAC addresses until that the trouble occurs at the authentication server 3, therefore the AP 2 can authenticate the MAC addresses by itself. Consequently, even when some troubles occur at the authentication server 3, the authentication procedure can be continued.

At a second embodiment of the present invention, the usable time of the shared key is limited to a designated period beforehand at a key control server (not shown), therefore the security is made to be high.

As shown in Fig. 5, at the S3 of the first embodiment, the STA 1 can always encrypt the challenge text received from the AP 2 by using the own shared key and the IV based on the WEP algorithm. At the second embodiment, in order that the illegal authentication is not executed even when the shared key is leaked, a security can be kept by limiting the usable time of the shared key.

Next, a third embodiment of the present invention is explained. At the second embodiment of the present invention, the usable time of the shared key for the WEP is limited, with this, the security against the illegal usage can be kept. However, when a legal user did not use the STA 1 within the usable limit time, the key must be transported in case that the legal user uses after the usable time limit.

At the third embodiment, an authentication method, at the time when the shared key becomes invalid due to the usable time limit, is explained.

Fig. 6 is a sequence diagram showing an authentication procedure of the third embodiment of the authentication method of the wireless LAN system of the present invention.

In Fig. 6, when the shared key from the STA 1 becomes invalid (unsuccessful), the STA 1 requests again the authentication for the AP 2 by the open system authentication method (S14).

The AP 2 recognizes that the request is executed by the open system authentication method, and requests the authentication for the authentication server 3 by using the MAC address as the authentication ID (S15).

In this, the authentication server 3, for example, operates based on the RADIUS protocol defined at the RFC 2138 of the IETF.

And the MAC address is defined as a user name or a calling station ID on the authentication protocol (RADIUS)

The authentication server 3 (RADIUS) authenticates the MAC address, and after this, transmits a challenge text by using a procedure equivalent to the CHAP defined at the RFC 1994 in the IETF (S16).

At the CHAP, a message digest MD 5 is defined as a hashing method being one way. However, instead of the MD 5, one of the other hashing methods can be used.

The AP 2, received the challenge text from the authentication server 3, returns the CHAP response (hashed challenge text) to the authentication server 3 by hashing by the CHAP (S17).

When the authentication server 3 recognizes that a normal response is received by the CHAP, the authentication server 3 notifies the AP 2 to the authentication completion as the total authentication is completed (S18).

The AP 2 received the information of the authentication completion notifies the authentication completion to the STA 1, and the STA 1 recognizes that the authentication is successful (S19).

After this, the STA 1 and the AP 2 go to the operation of association (S20).

When the authentication between the AP 2 and the authentication server 3 was successful, as mentioned at the first embodiment, the newly authenticated MAC address can be registered in the usable MAC address table stored in the AP 2. However, at the third embodiment, the open system authentication method is used and the security is low, therefore it is recommended that the newly authenticated MAC address is not newly registered.

After the association procedure is completed, the STA 1 executes communication by a normal IP (Internet protocol) packet through the AP 2.

Next a fourth embodiment of the present invention is explained. In case of the open system authentication method at the third embodiment, the communication period does not have a limit after the association, consequently, the possibility that an illegal connection is executed is high.

At the fourth embodiment of the present invention, an effective period of communication after the association is decided to a designated short period that is sufficient for that the shared key of the WEP algorithm is transported from a key control server (not shown) by using such an Internet Key Exchange method of Public Key Infrastructure. For example, this effective period of communication is recommended to be 10 seconds to one minute.

In Fig. 6, after the key is transported for the original shared key authentication method, de-association is executed (S21), and the connection is executed again by the shared key authentication method. As a result, even an illegal access used a false MAC address is executed, the security can be kept in high.

As mentioned above, at the present invention, the MAC address authentication, in which the shared key authentication method stipulated in the IEEE 802.11 is expanded, is executed. With this, at the wireless LAN system in which an illegal usage is liable to occur because of the usage of a wireless LAN card, the security can be kept in high. And the authentication for many wireless LAN cards can be executed from any of access points.

Moreover, at the present invention, a usable time limit of the shared key of the WEP is decided, and the period of the association at the open system authentication method is limited, consequently, the security can be kept in high.

Further, the MAC address table in the AP is automatically renewed by the instruction from the authentication server. Therefore, even the authentication server has some troubles, by utilizing the MAC address information until right before the troubles, the AP itself can authenticate the MAC address.

While the present invention has been described with reference to the particular illustrative embodiments, it is not to be restricted by those embodiments but only by the appended claims. It is to be appreciated that those skilled in the art can change or modify the embodiments without departing from the scope and spirit of the present invention.